REMARKS/ARGUMENTS

1.) Claim Amendments

The Applicant has amended claims 1, 3, 10-11, 16-18, 20, 27, and 29; claims 4, 15, and 21 have been canceled; claims 32-33 have been added. Applicant respectfully submits no new matter has been added. Accordingly, claims 1-3, 5-14, 16-20, 22-33 are pending in the application. Favorable reconsideration of the application is respectfully requested in view of the foregoing amendments and the following remarks.

2.) Claim Rejections – 35 U.S.C. § 103 (a)

Claims 1-31 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Niemi, *et al.* (RFC 3310, HTTP Digest Authentication Using AKA) in view of Reiche (US 6,092,196) and further in view of Tuomi, *et al.* (US 7,395,050). Applicants respectfully traverse the Examiner's rejection and have further amended the independent claims to more clearly and distinctly claim the subject matter which the Applicants consider as their invention. In view of the above amendments and the following remarks, a favorable reconsideration is earnestly requested.

For the Examiner's review, now amended independent Claim 1 is reproduced below:

1. A method of generating a password for use by an end-user device (UE) to access a remote server, comprising:

A) sending a request for access from the UE to the remote server;

B) creating a temporary identity for the UE by said remote server;

C) sending to an authentication node in the UE's home network details of the request for access, said details including said temporary identity for the UE;

D) at the authentication node or the remote server, generating a Hypertext Transfer Protocol (HTTP) Digest challenge to said UE using an algorithm capable of generating end-user password, including details of the temporary identity of the UE and identity of said remote server;

E) at the UE, generating a password based on the HTTP Digest challenge, said password being associated with the identity of the remote server and the identity of the UE;

F) storing the password and the temporary identity of the UE at the UE; and

G) sending an authentication response from said UE including said temporary identity and a proof of possession of the password thereby establishing authentication between said UE and said remote server.

In accordance with the teachings of the present invention, in response to receiving an access request from an end-user device (UE), the remote server creates a temporary identity for the requesting UE (steps A & B above). The Examiner stated that such step of a remote server creating a temporary identity for the requesting UE is disclosed in Tuomi (Col. 10, lines 59-61). However, in Tuomi, it is clearly stated that it is the authentication server (114 of Fig. 3 in Tuomi) that creates the user ID for the user. Accordingly, Tuomi fails to disclose or teach a remote server which is separate and different from an authentication server (or authentication node as described in the present application) creating a temporary identity in response to receiving an access request from an UE. After an initial authentication of the UE with the help of the authentication node in the UE's home network as recited in independent claim 1, in accordance with the teachings of the present invention and as further claimed in dependent claim 32, in order to enable the remote server to directly authenticate the UE for any subsequent access requests, it is the remote server which has to create the temporary identity for the requesting UE. As a result, Tuomi's authentication server assigning a User ID for the user is distinguishable from the presently recited invention.

Because Tuomi fails to anticipate or render obvious the recited step of creating a temporary identity for the UE, Tuomi, independent or in combination with other references, also fails to anticipate or render obvious recited step (C) of "sending to an authentication node in the UE's home network details of the request for access, said details including said temporary identity for the UE." In that regard, Reiche further cited by the Examiner likewise fails to disclose or teach the step of sending details of the access request to the home network's authentication node wherein such details include the temporary identity for the UE as created by the remote server. In Reiche, it merely shows the customer server redirecting a web access from a particular user to the authentication server associated that that user's home network. However, nothing in

Reiche discloses or teaches the step of sending details of the access request wherein such details include a temporary identity for the UE as created by the remote server.

The Examiner then incorrectly stated that step (D) of "generating a HTTP challenge using an algorithm capable of generating end-user passwords, including details of the temporary identity of the UE" is disclosed by Niemi on Pages 6 and 7. Applicants respectfully disagree with the Examiner's rejection since Niemi discloses generating a HTTP challenge using a shared secret key (K) which has been established beforehand between the ISIM in the UE and the Authentication Center (AC). Accordingly, there is nothing in Niemi that discloses generating a HTTP challenge using the temporary identity created by the remote server. Moreover, in order to expedite the allowance, Applicants has further amended independent Claim 1 to recite that such HTTP challenge is generated to the UE using an algorithm capable of generating end-user password, including details of the temporary identity of the UE and the identity of the remote server as well.

The Examiner then maintained his previous rejection that recited steps (E and F) wherein "at the UE, generating a password based on the HTTP Digest challenge, said password being associated with the identity of the remote server and the identity of the UE and storing the password and the temporary identity of the UE at the UE" are somehow disclosed by Reiche (Col. 5-6). As previously argued by the Applicant, in Reiche, it simply issues control data to the client's machine to display a regular "log on box" in which the client can then type in his or her user id and password. There is nothing in Reiche disclosing or teaching an UE generating a password based on the HTPP Digest challenge wherein such generated password is associated with the identity of the remote server and the identity of the UE.

In order to expedite the allowance of the pending claims, Applicants have further amended independent claim 1 to recite step (G) of "sending an authentication response from said UE including said temporary identity and a proof of possession of the password thereby establishing authentication between said UE and said remote server." Applicants submit that nothing in Niemi, Reiche, and/or Tuomi teaches or discloses the step of the UE sending an authentication response with the temporary identity created

by the remote server to enable the UE to authenticate with the remote server. Applicants therefore respectfully submit that now amended independent Claim 1 and its dependent claims 2-3, 5-14, 16-17, and 32 are now in condition for allowance. Claim 18 has now been rewritten into independent form and recite similar novel and unobvious steps. Therefore, independent Claim 18 and its dependent claims 19-20, 22-31, and 33 are also in condition for allowance.

CONCLUSION

In view of the foregoing remarks, the Applicant believes all of the claims currently pending in the Application to be in a condition for allowance. The Applicant, therefore, respectfully requests that the Examiner withdraw all rejections and issue a Notice of Allowance for all pending claims.

The Applicant requests a telephonic interview if the Examiner has any questions or requires any additional information that would further or expedite the prosecution of the Application.

Respectfully submitted,

John C. Han
Registration No. 41,403

Date: August 12, 2009

Ericsson Inc.
6300 Legacy Drive, M/S EVR 1-C-11
Plano, Texas 75024

(972) 583-7686
john.han@ericsson.com